UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/666,160	09/19/2003	Daryl Carvis Cromer	RPS920020026US1	7087

25299　7590　12/20/2006	EXAMINER
IBM CORPORATION PO BOX 12195 DEPT YXSA, BLDG 002 RESEARCH TRIANGLE PARK, NC 27709	PATEL, NIRAV B

	ART UNIT	PAPER NUMBER
	2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/20/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/666,160	CROMER ET AL.
	Examiner	Art Unit
	Nirav Patel	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>19 September 2003</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-29</u> is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-29</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>19 September 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☐ All   b)☐ Some * c)☐ None of:

　　　　1.☐ Certified copies of the priority documents have been received.

　　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
　　Paper No(s)/Mail Date <u>9/19/03</u>.

4)☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

1. This action is in response to the application filed on 09/19/2003.

2. Claims 1-29 are under examination.

Specification

3. The disclosure is objected to because of the following informalities:

The specification is objected because they fail to show component number as described in the drawing **[Fig. 2, remote control → 46, last line of page 14 "remote control 60"].**

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 22-29 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 22 recites "A computer readable medium storing program code causing a microprocessor controlling a receiver to perform a method including: reading a hash value from data storage within said receiver, transmitting data indicating programming to be decrypted together with said hash value to a program provider; receiving a secret

code from said program provider; decrypting said secret code with a private cryptographic key stored in said data storage; and storing a decrypted form of said secret code for use to decrypt program content in said data storage". Claim 22 is rejected under 35 USC 101 for failing to provide a practical application that produces a useful, tangible and concrete result. From the **specification, page 12 last paragraph and page 13 lines 1-2**, it states "Instructions for programs to execute within the computer system 74 may also be provided in the form of a computer data signal embodied in a carrier wave". Based on the cited disclosure above, it is determined that the readable medium carrying a signal recites a non-statutory matter. Therefore, Claim 22 is rejected under 35 USC 101.

Claim 23 recites "A computer data signal embodied in a carrier wave comprising program code causing a microprocessor controlling a receiver to perform a method including: reading a hash value from data storage within said receiver, transmitting data indicating programming to be decrypted together with said hash value to a program provider; receiving a secret code from said program provider; decrypting said secret code with a private cryptographic key stored in said data storage; and storing a decrypted form of said secret code for use to decrypt program content in said data storage". **However, the signal is non-tangible subject matter and the claim is rendered as non-statutory.** Therefore, Claim 22 is rejected under 35 USC 101 for failing to provide a practical application that produces a useful, tangible and concrete result.

Claims 24 and 26 have limitation that are similar to those of claim 22, thus they are rejected with the same rationale applied against claim 22 above.

Claim 27 depend on claim 26, therefore they are rejected with the same rationale applied against claim 26 above.

Claim 25 and 28 have limitation that are similar to those of claim 23, thus they are rejected with the same rationale applied against claim 23 above.

Claim 29 depend on claim 28, therefore they are rejected with the same rationale applied against claim 28 above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 18, 22 and 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Ansell et al (US Patent No. 6,792,113).

As per claim 18, Ansell discloses:

a) generating a hash value within said receiver [col. 6 lines 9-16], wherein said hash value represents a computer readable serial number of a component within said receiver [col. 6 lines 5-9]; b) storing said hash value in data storage within said receiver [Fig. 1]; c) reading said hash value from data storage, d) transmitting data indicating programming to be decrypted together with data identifying said receiver and said hash value to a program provider [Fig. 6B], e) finding a data record within a database accessed by said program provider including said data identifying said receiver [col. 14 lines 29-44]; f) matching said hash value transmitted from said receiver with a hash value stored within said data record [col. 14 lines 40-44]; g) generating a secret code identifying said programming to be decrypted [Fig. 4 or 5]; h) encrypting said secret code with a public cryptographic key of said receiver stored within said data record to form an encrypted version of said secret code [Fig. 4 or 5]; i) transmitting said secret code from said program provider to said receiver; k) decrypting said encrypted secret code within said receiver with a private cryptographic key stored within said receiver; and l) decrypting said portion of said program content with said secret code within said receiver [Fig. 4 or 5, 3A or 3B, 2, 1].

As per claim 22, it encompasses limitations that are similar to limitations of claim 19. Thus, it is rejected with the same rationale applied against claim 18 above.

As per claim 23, it encompasses limitations that are similar to limitations of claim 19.

Thus, it is rejected with the same rationale applied against claim 18 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3, 6, 7 and 8 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ansell et al (US Patent No. 6,792,113) and in view of Pearce et al

(US Patent No. 6,243,468).

As per claim 1, Ansell discloses:

a receiver comprises:

a component identified by a computer readable serial number [col. 6 lines 5-9], data

storage storing access data determining programming to be decrypted by said receiver,

a public cryptographic key, a private cryptographic key for decrypting information

encrypted with said public cryptographic key, and a code representing said component

identifier [Fig. 1, component 104, Fig. 22-24, Fig. 2], and a signal processor decrypting

said encrypted program content in accordance with said access data stored within said

data storage [col. 6 lines 44-47, Fig. 2]; and a first microprocessor [Fig. 1 component 104], a first method comprising: reading said computer readable serial number; generating a hash value representing said computer readable serial number, and storing said hash value in said data storage [Fig. 1, component 104, col. 6 lines 5-16], said receiver additionally performs a second method comprising: reading said hash value from said data storage, transmitting data indicating programming to be decrypted together with said hash value to a program provider [Fig. 1, 6B, col. 14 lines 22-28], and said receiver additionally performs a third method comprising: receiving a secret code from said program provider; decrypting said secret code with said private cryptographic key stored in said data storage; and storing a decrypted form of said secret code as said access data in said data storage [Fig. 6B, 4, 5, col. 12 lines 63-65, col. 9 lines 48-51, Fig. 3A, 3B].

Ansell teaches generating a hash value representing said computer readable serial number [col. 6 lines 5-16]. Ansell doesn't expressively mention periodically performs the first method (i.e. generating a hash value).

Pearce teaches generating a hash value periodically [Fig. 5, col. 6 lines 64-67].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Pearce with Ansell, since one would have been motivated to prevent piracy or illicit use of the content [Pearce, col. 1 lines 6-7].

As per claim 3, the rejection of claim 1 is incorporated and Ansell discloses:

said data storage additionally stores a digital certificate, and said digital certificate is transmitted with said data indicating programming to be decrypted [Fig. 1, 23, 6B].

As per claim 6, the rejection of claim 1 is incorporated and Ansell discloses:

said second method additionally includes transmitting transaction data for purchasing additional program content [Fig. 8, col. 15 lines 30-35, col. 3 lines 1-5].

As per claim 7 and 8, the rejection of claim 1 is incorporated and Ansell discloses:

a portion of information transmitted to said program provider during performance of said second method is encrypted with a private key of said receiver/ a public key of said program provider [col. 7 lines 20-30, Fig. 6B].

7. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al (US Patent No. 6,792,113) in view of Pearce et al (US Patent No. 6,243,468) and in view of Russ et al (US Patent No. 6,748,080).

As per claim 2, the rejection of claim 1 is incorporated and Ansell discloses the processor and the data storage for storing the hash value and reading/writing the hash value [Fig. 1] and transmits the data indicating programming to be decrypted together with the hash value to the program provider [Fig. 6B]. Pearce teaches generating a hash value periodically [Fig. 5, col. 6 lines 64-67]. Ansell and Pearce don't expressively mention a second microprocessor.

However, Russ teaches a second microprocessor [Fig. 3 → 314 i.e. secure element to access the private data in the memory 704], a first processor [Fig. 312, which communicates with the secure element and the secure element provides the data to the processor], a read-only key register storing said private key and a program control register (memory) [Fig. 3 or 9 component 314, 312, Fig. 7 → 314, which provides the memory (704) read/write operation].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Russ with Ansell and Pearce to include the second processor (i.e. secure element), since one would have been motivated to provide the security for the operators/receivers of the subscriber network system [Russ, col. 2 lines 11-14].

8. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al (US Patent No. 6,792,113) in view of Pearce et al (US Patent No. 6,243,468) and in view of Ellis (US Patent No. 7,086,086).

As per claim 4, the rejection of claim 1 is incorporated and Ansell discloses:

a plurality of components identified by computer readable serial numbers [col. 6 lines 10-16]. Ansell teaches storing the hash value and transmitting data indicating programming to be deciphered together with said hash value to said program provider [Fig. 1, 6B].

Ellis teaches generating a hash value representing each of said computer readable

serial numbers [col. 10 lines 58-61].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to combine Ellis with Ansell and Pearce, since one would have

been motivated to authenticate the device (i.e. receiver) [Ellis, col. 10 lines 64-67].

9.   Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et

al (US Patent No. 6,792,113) in view of Pearce et al (US Patent No. 6,243,468) and in

view of Gilley et al (US Patent No. 5,771,287).

As per claim 5, the rejection of claim 1 is incorporated and Gilley discloses generating

authentication code (i.e. hash) periodically [col. 4 lines 17-25]. Further, Gilley teaches

performing the first method (i.e. generating the hash/authentication code) whenever the

receiver is turned on [col. 4 lines 17-25].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to combine Ellis with Ansell and Pearce, since one would have

been motivated to resist the tempering of hardware from the system/device [Ellis, col. 1

lines 10-12, col. 3 lines 29-30].

10. Claims 9-13, 17, 19, 24, 25, 26 and 28 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Ansell et al (US Patent No. 6,792,113) and in view of Akiyama

et al (US Pub. 2003/0002679).

As per claim 9, Ansell discloses:

input means for receiving data signals from each receiver [Fig. 1, 6B]; output means for

transmitting a secret code indicating a portion of said encrypted programming to be

displayed by each receiver [Fig. 6B, 4, 5, 2]; data storage; a processor; and a database

storing a data record for each receiver in said plurality of receivers, wherein each said

data record includes a first data field identifying an address for sending data to said

receiver, a second data field for storing a hash value for said receiver, and a third data

field for storing a public cryptographic key of said receiver [Fig. 1, component 102, col.

10 lines 45-67, col. 11 lines 31-40].

Akiyama teaches plurality of receivers and transmits the secret code indicating a portion

of said encrypted programming to be displayed by each receiver in said plurality of

receivers [paragraph 0013, Fig. 1, 10, 14].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to combine Akiyama with Ansell, since one would have been

motivated to provide the conditional access to the content [Akiyama, paragraph 0011

lines 2-3].

As per claim 10, the rejection of claim 9 is incorporated and Ansell discloses:

receiving a message from a receiver in said plurality of receivers including data identifying said receiver, data indicating programming to be decrypted by said receiver, and a hash value [Fig. 6B]; identifying a data record within said database from said data identifying said receiver, determining said hash value received in said message matches said hash value stored in said data record [col. 14 lines 39-45], generating a secret code identifying programming to be decrypted by said receiver, encrypting said secret code with a public cryptographic key of said receiver stored in said data record to form an encrypted version of said secret code; and transmitting said encrypted version of said secret code to said receiver [Fig. 4 or 5, Fig. 1].

As per claim 11, the rejection of claim 9 is incorporated and Ansell teaches said data record, which comprises the key record [Fig.1, 19].
Akiyama teaches:

storing said secret code in the data record [Fig. 5 or 6].

As per claim 12, the rejection of claim 10 is incorporated and is rejected for the same reason set forth in the rejection of claim 9 above. Further, Akiyama teaches plurality of receivers [paragraph 0013].

As per claim 13, the rejection of claim 12 is incorporated and is rejected for the same reason set forth in the rejection of claim 11 above. Further, Akiyama teaches plurality of

receivers, the contracting user database and channel key/seed database [paragraph 0013 Fig. 2, 3].

As per claim 17, the rejection of claim 12 is incorporated and Ansell discloses:

said second method additionally includes transmitting transaction data for purchasing additional program content [Fig. 8, col. 15 lines 30-35, col. 3 lines 1-5].

As per claim 19, the rejection of claim 18 is incorporated and Ansell discloses transmitting said public cryptographic key of said receiver, and said hash value from said receiver to said program provider [Fig. 6B, 1]; establishing an additional data record within said database accessed by said program provider; and storing said data indicating said receiver is to be registered with said program provider, said public cryptographic key of said receiver, and said hash value from said receiver in said additional data record [Fig. 17, col. 10 lines 45-63].

Akiyama teaches:

transmitting data indicating said receiver is to be registered with said program provider [Fig. 7, 3, paragraph 0112].

As per claim 24, it encompasses limitations that are similar to limitations of claim 10. Thus, it is rejected with the same rationale applied against claim 10 above.

As per claim 25, it encompasses limitations that are similar to limitations of claim 10. Thus, it is rejected with the same rationale applied against claim 10 above.

As per claim 26, it encompasses limitations that are similar to limitations of claims 10 and 19. Thus, it is rejected with the same rationale applied against claim 10 and 19 above.

As per claim 28, it encompasses limitations that are similar to limitations of claim 26. Thus, it is rejected with the same rationale applied against claim 26 above.

11. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al (US Patent No. 6,792,113) in view of Akiyama et al (US Pub. 2003/0002679) and in view of Khandelwal et al (US Patent No. 6,993,132).

As per claim 14, the rejection of claim 12 is incorporated and Ansell teaches:

data storage storing a data structure including hash values [col. 10 lines 45-50, col. 11 lines 31-35]; said second method additionally includes determining that said hash value matches a hash value within said plurality of hash values before transmitting said encrypted version of said secret code identifying programming to be decrypted by said additional receiver to said additional receiver [col. 14 lines 40-45, Fig. 6B].

Khandelwal teaches the hash value received from one or more manufacturers of said receivers [col. 3 lines 22-27, col. 5 lines 3-7].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Khandelwal with Ansell and Akiyama, since one would have been motivated to prevent fraudulent access in digital cable networks [col. 1 lines 8-9].

As per claim 15, the rejection of claim 14 is incorporated and Ansell teaches:

said second method additionally includes determining validity of a digital certificate in which said public cryptographic key is transmitted [Fig.19 col. 11 lines 31-34, 41-45].

12. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al (US Patent No. 6,792,113) in view of Akiyama et al (US Pub. 2003/0002679) and in view of Ellis (US Patent No. 7,086,086).

As per claim 16, the rejection of claim 12 is incorporated and Ansell discloses:

said second data field stores a first of hash values for said receiver [Fig. 19 col. 11 lines 31-35], said first method includes receiving a second of hash value within said message from said receiver and determining whether said each of said second of hash value matches a hash value within said first of hash values [col. 14 lines 40-45], and said second method includes receiving a third hash value within said message from said additional receiver and storing said third plurality of hash values in said additional data record [Fig. 6B, 19].

Akiyama teaches plurality of receiver (i.e. additional receiver) [Fig. 1, paragraph 0013].

Ellis teaches generating a hash value representing each of said computer readable

serial numbers (i.e. plurality of hash values) [col. 10 lines 58-61].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to combine Ellis with Ansell and Akiyama, since one would

have been motivated to authenticate the device (i.e. receiver) [Ellis, col. 10 lines 64-67].

13. Claims 20, 27 and 29 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ansell et al (US Patent No. 6,792,113) in view of Akiyama et al (US

Pub. 2003/0002679) in view of Khandelwal et al (US Patent No. 6,993,132) and in view

of Ellis (US Patent No. 7,086,086).

As per claim 20, the rejection of claim 19 is incorporated and Ansell teaches:

storing said plurality of hash values in a data structure accessed by said program

provider [Fig. 17, col. 10 lines 45-50, col. 11 lines 31-35]; determining that said hash

value matches a hash value within said plurality of hash values [col. 14 lines 40-45, Fig.

6B].

Khandelwal teaches the hash value received from one or more manufacturers of said

receivers [col. 3 lines 22-27, col. 5 lines 3-7].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to combine Khandelwal with Ansell and Akiyama, since one

would have been motivated to prevent fraudulent access in digital cable networks [col. 1

lines 8-9].

Ellis teaches generating a hash value representing each of said computer readable serial numbers (i.e. plurality of hash values) [col. 10 lines 58-61].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Ellis with Ansell and Akiyama, since one would have been motivated to authenticate the device (i.e. receiver) [Ellis, col. 10 lines 64-67].

As per claim 27, it encompasses limitations that are similar to limitations of claim 20. Thus, it is rejected with the same rationale applied against claim 20 above.

As per claim 29, it encompasses limitations that are similar to limitations of claim 20. Thus, it is rejected with the same rationale applied against claim 20 above.

14. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ansell et al (US Patent No. 6,792,113) in view of Akiyama et al (US Pub. 2003/0002679) in view of Khandelwal et al (US Patent No. 6,993,132) in view of Ellis (US Patent No. 7,086,086) and in view of Gilley et al (US Patent No. 5,771,287).

As per claim 21, the rejection of claim 20 is incorporated and Gilley discloses generating authentication code (i.e. hash) periodically [col. 4 lines 17-25]. Further, Gilley teaches performing during initialization each time power is turned on at the receiver [col. 4 lines 17-25].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Ellis with Ansell and Pearce, since one would have been motivated to resist the tempering of hardware from the system/device [Ellis, col. 1 lines 10-12, col. 3 lines 29-30].

Conclusion

15.The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Oka et al (US 2004/0039911) --- Content usage authority management system and management method

Mineo (US 2001/0056493) --- Server assignment device, service providing system and service providing method

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP

12/8/06

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100